

Annual 47 C.F.R. §64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual 47 C.F.R. §64.2009(e) CPNI Certification covering the prior calendar year 2018.

Date Filed: February 15, 2019

Company Name: West IP Communications, Inc.

Form 499 Filer ID: 826161

Name of signatory: Randall McGraw

Title of signatory: President, Global Portfolio Management

I, Randall McGraw, certify that I am an officer of West IP Communications, Inc. (“WIPC”), and acting as an agent of WIPC, that I have personal knowledge that WIPC has established operating procedures that are adequate to ensure compliance with the Commission’s CPNI rules. *See* 47 C.F.R. §64.2001 *et seq.*

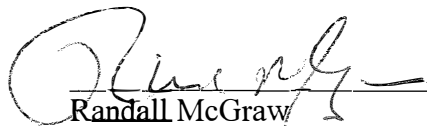
Attached to this certification is an accompanying statement explaining how WIPC’s procedures ensure that WIPC is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission’s rules.

WIPC has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at state commissions, the court system, or at the Federal Communications Commission) against data brokers in the past year.

WIPC has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

WIPC represents and warrants that the above certification is consistent with 47 C.F.R. §1.17, which requires truthful and accurate statements to the Commission. WIPC also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed:



Randall McGraw
President, Global Portfolio Management
West IP Communications, Inc.

Accompanying Statement to Annual 47 C.F.R. §64.2009(e) CPNI Certification

West IP Communications, Inc. (“WIPC”) has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission’s (“FCC”) rules pertaining to customer proprietary network information (“CPNI”) set forth in sections 64.2001 – 64.2011 of the Commission’s rules. This attachment summarizes those practices and procedures.

1. Identification of CPNI. WIPC has established procedures to identify what customer information is CPNI consistent with the definition of CPNI under 47 C.F.R. § 64.2003(g) and 47 U.S.C. § 222(h)(1).

2. Uses of CPNI Not Requiring Customer Approval. WIPC has established procedures to identify uses of CPNI that do not require customer approval under 47 C.F.R. § 64.2005 and 47 U.S.C. § 222(c)-(d). WIPC may use CPNI without customer approval to (a) initiate, render, repair, maintain, bill, troubleshoot, and collect for services provided by WIPC, (b) protect WIPC’s rights and property or to protect its subscribers or other carriers from the unlawful or fraudulent use of WIPC’s services, (c) provide call location information required in connection with emergency services, (d) market services formerly known as adjunct-to-basic services, (e) market WIPC’s services within the categories of services to which the customer already subscribes, and (f) respond to a valid request from law enforcement, a court order, or other appropriate authority.

3. Uses of CPNI Requiring Customer Approval. WIPC has established procedures to identify uses of CPNI requiring customer approval under 47 C.F.R. § 64.2007 and how to properly obtain approval to use, disclose, or access CPNI under the Opt-Out, Opt-In, and One-Time Use notification methods under 47 C.F.R. § 64.2008.

4. Procedures Protecting Against Disclosure of CPNI. WIPC has established procedures to protect against the disclosure of CPNI, in accordance with 47 C.F.R. § 64.2010, including without limitation: (a) authentication of customers before disclosing CPNI on customer-initiated calls, (b) instructing customers who request Call Detail Information on inbound calls to access such information through an online portal controlled by password, and (c) implementing procedures to provide immediate notification to customers of account changes.

5. Record-Keeping Requirements. WIPC has established procedures on CPNI record-keeping requirements under 47 C.F.R. §§ 64.2008(a)(2), 64.2009 and 64.2010(d). The WIPC CPNI Policy Administrator is required to collect and maintain records related to any (a) CPNI security breach for at least two years, (b) efforts to obtain approval to use, disclose, or access CPNI under the Opt-Out, Opt-In, and One-Time Use notification methods for at least one year, and (c) sales and marketing campaign that uses CPNI for at least one year.

6. Reporting Requirements. WIPC has established procedures on CPNI reporting requirements under 47 C.F.R. §§ 64.2009(f) and 64.2011. WIPC employees are required to immediately report (a) any unauthorized disclosure, use, or access of CPNI or breach of any database containing CPNI, and (b) any malfunction in WIPC’s use of the Opt-Out notification

method for obtaining customer approval to use, disclose, or access CPNI. In the event of a CPNI security breach, WIPC will comply with all applicable breach notification laws.

7. Training and Disciplinary Process. WIPC employees having access to, or occasion to use CPNI, are required to receive training on CPNI, which includes instruction on when they are and are not authorized to use CPNI under 47 C.F.R. § 64.2009(b). WIPC also has in place an express disciplinary process to address any unauthorized use, disclosure, or access of CPNI pursuant to 47 C.F.R. § 64.2009(b).

8. Additional Safeguards. WIPC has developed additional safeguards to protect CPNI, including (a) requiring its employees to verify prior opt-in or opt-out customer approval before using, disclosing, or accessing CPNI, (b) prohibiting WIPC employees from providing customers with lost passwords over the telephone, (c) requiring independent contractors and joint venturers to enter into confidentiality agreements, (d) prohibiting all third parties from using CPNI for marketing purposes, (e) requiring prior approval by the CPNI Policy Administrator of all vendor contracts that will result in the disclosure of WIPC customer CPNI, (f) prohibiting WIPC employees from using proprietary information obtained from other carriers for purposes not intended by such carriers, (g) prohibiting WIPC employees from using, disclosing, or permitting access to CPNI to identify or track customers that call competing service providers, and (h) establishing a supervisory review process for sales and marketing campaigns that use customer CPNI.